Segmentação de Redes com VLAN

Leonardo Haffermann

Pós Graduação em Redes e Segurança de Sistemas
Pontifícia Universidade Católica do Paraná

Curitiba, Novembro de 2009

Resumo

Este artigo foi desenvolvido com o intuito de aprofundar os conhecimentos referentes a implementação de Redes Locais Virtuais (Vlan), destinada a obtenção de uma segmentação lógica (virtual) em um ambiente físico a fim de se obter melhor desempenho e segurança em uma estrutura de rede corporativa. Através do estudo de suas diversas características e configurações pode-se obter o conhecimento necessário para comparar as diferentes formas de implementação de Vlans e, de certa forma, dominar esta tecnologia que vem se destacando nos últimos anos por sua economia, flexibilidade e versatilidade.

1 Introdução

Nos últimos anos a velocidade e a quantidade das informações que trafegam pela grande Rede têm experimentado um crescimento que não tende mais a regredir. O mesmo ocorre, em escala menor, na rede local de uma organização, onde um número crescente de computadores, periféricos (impressoras, scanners, câmeras, telefonia voip, etc) e servidores que fornecem serviços e sistemas diversos compartilham o mesmo meio de comunicação gerando um nível de tráfego na rede que, se não corretamente gerenciado pode ocasionar lentidão ou até mesmo a indisponibilidade de um ou mais serviços.

A implantação de VLANs (Virtual Local Área Network) tem a intenção de segmentar uma rede lógica afim de aumentar o controle de tráfego da rede, diminuir o alcance de disseminação de pacotes de difusão (broadcast) e de pragas virtuais, melhorado assim o desempenho e a segurança de uma determinada rede.

Inicialmente serão apresentados os riscos e problemas provenientes do uso de uma rede não segmentada. Em seguida será exposto o conceito de VLAN para, na sequencia, aprofundar-se no estudo das características, classificação e configuração das VLANs. Finalmente será apresentado um comparativo das tecnologias estudadas sob o enfoque da segurança, gerenciamento e qualidade do serviço.

2 Descrição detalhada do problema

Atualmente é cada vez mais comum o uso de soluções virtuais, disponíveis a um clique, para substituir ações que, há pouco tempo, eram efetuadas fisicamente demandando deslocamentos e tempo disponível como por exemplo em livrarias online onde podem-se adquirir livros, físicos ou virtuais, em pouco tempo sem a necessidade de sair de sua

residência. Em uma organização esta tendência segue o mesmo caminho afim de agilizar processos, diminuir custos e aumentar lucros.

Este aumento de soluções e, consequentemente, de informações trafegando pela rede trouxe uma nova preocupação para a equipe de TI (Tecnologia da Informação) que é o congestionamento dos links. O crescimento desenfreado do tráfego de rede cria gargalos em determinados pontos da estrutura, podendo gerar lentidão ou até tornar alguns serviços indisponíveis temporariamente. Esta situação pode ser agravada pela propagação de pacotes de difusão (broadcast) que em muitos casos consomem fatia considerável da banda de um enlace de dados.

Outra questão importante a se considerar é a segurança. Com o aumento de informações confidenciais circulando pela rede cresce também o interesse de pessoas mal intencionadas buscando capturar dados para fins diversos por meio da disseminação de pragas virtuais (vírus, worms, malwares, etc) ou através de sniffers, capturando pacotes e extraindo dados que lhe pareçam interessantes para uso futuro.

3 LAN, Segmentação e VLAN

Uma rede local (LAN) pode ser definida como uma área de comunicação de dados interligada de abrangência restrita e altas taxas de transmissão, porém é mais comumente descrita como sendo um domínio de broadcast, isto porque, um pacote de difusão lançado em uma rede local dissemina-se para todos os pontos de acesso ativos.

A Segmentação de Redes surgiu para, entre outros motivos, limitar a disseminação de broadcasts em uma rede local e consiste em inserir dispositivos na rede (roteadores) que bloqueiam a passagem de pacotes de broadcasts quando atravessam suas interfaces. Estes roteadores têm também a função de interligar diferentes Lans.

Mais informações a respeito de Redes Locais e Segmentação de Redes podem ser encontradas em “Conhecimentos Básicos de Redes” [6].

No entanto, para se obter o mesmo nível de segmentação e segurança de uma rede local pode se utilizar uma solução de baixo custo, se comparado com os preços dos roteadores, através de Vlans (Virtual Local Área Network). Uma Vlan proporciona uma segmentação lógica da rede através de comutadores (bridges ou switches) com esta função.

Uma atributo importante das Vlans é o fato de poder usá-la “onde existe a necessidade de separar a topologia lógica de segmentos de rede da topologia física” [3]. Pode se ativar duas Vlans em algumas portas de diferentes switches, fazendo com que estas se comportem como duas redes separadas, sendo assim, todos os pacotes provenientes de dispositivos membros de uma Vlan somente serão encaminhados para as portas dos switches pertencentes a mesma Vlan. Um exemplo básico de uma Vlan é apresentado na figura abaixo.

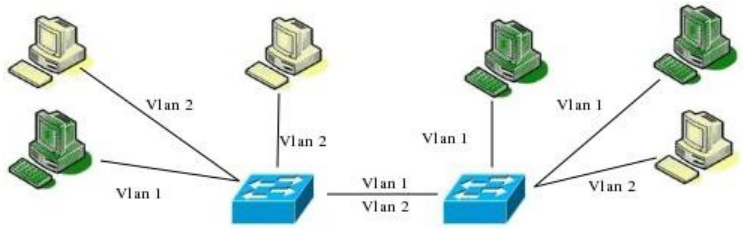

Figura 1: Exemplo de Vlan

A implementação do conceito de Vlans torna o gerenciamento das redes locais mais flexíveis levando em consideração o fato de permitir que computadores possam fazer parte de

uma ou outra Vlan sem que seja necessário alterar a organização física da rede. Por outro lado, em sua configuração básica, computadores de uma Vlan não podem se comunicar com computadores de outra Vlan, da mesma forma como redes locais diferentes não podem se comunicar. Assim também como nas redes locais, nas Vlans devem ser usados dispositivos roteadores para proporcionar a interconectividade entre estas. O roteamento entre Vlans será analisado mais adiante. Na figura abaixo podemos ver um exemplo de interligação de Vlans usando roteadores.

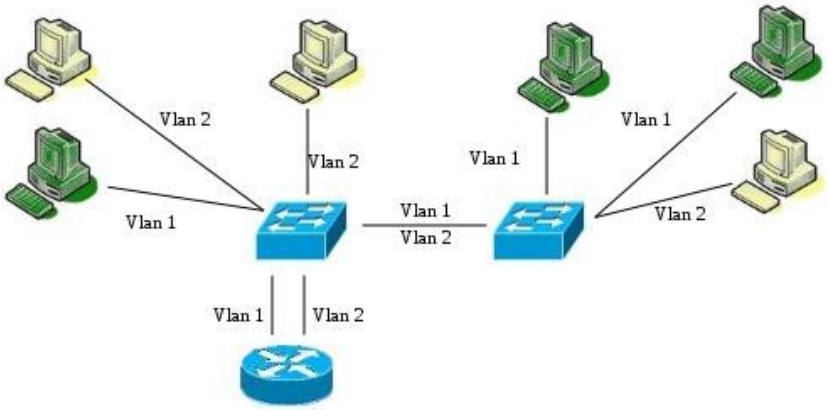

Figura 2: Interconexão entre Vlans

3.1 Características das VLANs

A principal característica atribuída ao uso de Redes Locais Virtuais é a possibilidade de se agrupar estações pertencentes a uma ou mais Lans físicas para se formar um único domínio de difusão ou Broadcast, garantindo a comunicação entre elas mesmo que façam parte de segmentos físicos diferentes [9].

Além desta existem outras características importantes quando se avalia o uso de Vlans que serão abordadas nos tópicos a seguir.

3.1.1 Controle de pacotes de difusão (broadcasts)

Em uma rede não segmentada, computadores, impressoras e outros dispositivos conectados disseminam uma grande quantidade de pacotes de difusão, seja por falhas na conexão dos cabos, mau funcionamento de placas de rede, ou até mesmo por protocolos e aplicações que geram este tipo de tráfego, podendo causar atraso no tempo de resposta e lentidão na rede local. No modelo de Vlans, existe um domínio lógico de difusão por onde os pacotes de broadcast ou multicast são contidos e não se propagam a outras redes virtuais [11]. Assim uma rede segmentada com Vlans cria vários subdomínios de difusão, diminuindo o tráfego de mensagens de difusão tanto na rede segmentada como na rede da organização em geral. A seguir podemos ver na figura como se comporta o tráfego de broadcasts em uma rede segmentada com Vlan.

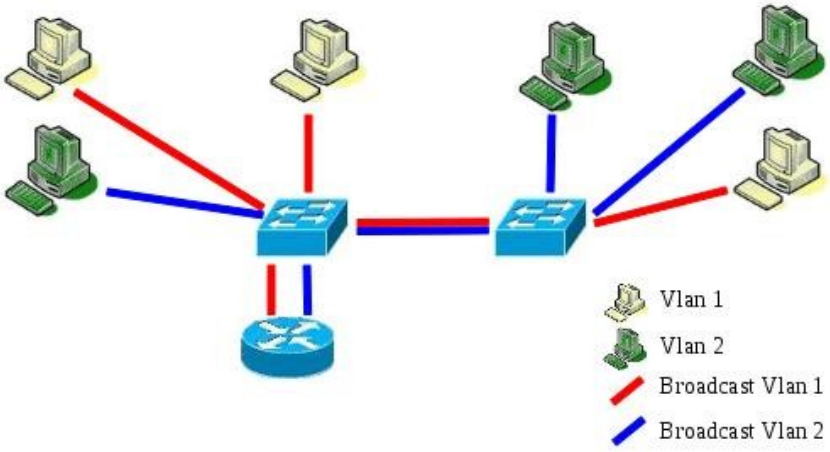

Figura 3: Disseminação de broadcasts com Vlan

3.1.2 Gerenciamento da rede

Em uma Lan comum, quando é necessário mudar um computador de um edifício para outro, com uma rede separada, é necessário executar uma série de procedimentos, desde lançamento de novo cabeamento, até configuração de rotas e regras para que o equipamento permaneça na mesma rede ligada anteriormente. Com Vlans, basta realizar a configuração dos comutadores e roteadores para que, em determinadas portas, seja permitido o tráfego de pacotes da Vlan a qual o equipamento pertencia anteriormente, o que evita perda de tempo com deslocamentos e instalações, proporcionando uma alta flexibilidade.

Os equipamentos que suportam o uso de Vlans também possuem funções de monitoramento de tráfego e comporta a ativação/desativação de portas permitindo que o administrador bloqueie portas que apresentem qualquer problema ou impedir que pessoas, inadvertidamente, conectem equipamentos em determinada rede virtual.

3.1.3 Performance da rede

A implementação de Vlan para segmentar uma rede melhora a performance. Como relatado anteriormente, os broadcasts e multicasts são confinados a Vlan onde trafegam evitando congestionamentos. Outra característica é o fato de diminuir o número de estações que compartilham o mesmo canal lógico diminuindo o tempo de acesso[5].

3.1.4 Segmentação lógica da rede

A implantação de redes virtuais pode ser aplicada de acordo com grupos de trabalhos ou setores mesmo que estes grupos estejam em localizações físicas distintas, garantindo assim a segmentação lógica da rede. Em determinada organização o setor financeiro pode pertencer a uma Vlan diferente do restante da organização a fim de proteger informações sigilosas. Em outra situação um setor que gera muito tráfego de rede pode fazer parte de outra Vlan a fim de melhorar o desempenho da rede de modo geral.

3.1.5 Segurança

A segurança é uma das características que mais é levada em conta quando se implementa Vlans, permitindo que dispositivos localizados em diferentes segmentos físicos e em uma mesma Vlan possam se comunicar sem que dispositivos fisicamente vizinhos tenham acesso [11]. Os pacotes transmitidos são normalmente entregues somente ao endereço de destino dificultando a interceptação dos mesmos. Quando se trata de tráfego entre Vlans, os pacotes são submetidos a um roteador, que possui diversas funcionalidades de filtragem, segurança e prioridade, antes de chegarem a seu suposto destino, criando assim domínios de segurança para acesso a recursos da rede.

3.1.6 Redução de Tempo e Custo

O uso de roteadores dedicados para realizar a interconexão de redes locais pode tornar os custos de segmentação de redes proibitivos. O uso de comutadores combinado com Vlans pode tornar a implementação mais atrativa se considerada a questão monetária.

Mas um custo ainda maior a médio e longo prazo pode se referenciar ao tempo despendido para reconfigurações físicas e migrações de dispositivos entre locais físicos, grupos ou redes locais diferentes. Usando-se Vlans as migrações e reconfigurações são realizadas em nível de software, através da console de gerenciamento dos switches.

3.2 Classificação das VLANs

As Redes Locais Virtuais podem ser classificadas de acordo com seu agrupamento, isto é, a forma como serão reunidos os dispositivos que farão parte das mesmas Vlans. Estes agrupamentos podem ser definidos por intermédio das portas do comutador, pelos endereços físicos das interfaces de rede, endereço IP dos clientes, endereços IP multicast, protocolos e também por uma combinação de alguns destes. Nas subseções a seguir os tipos de agrupamentos serão apresentados com mais detalhes.

3.2.1 Agrupamento por portas

Este tipo de agrupamento leva em conta apenas as portas do switch, não considerando os dispositivos, utilizador ou sistema conectados à outra ponta. Neste modelo cada porta do switch é associada a uma ou mais Vlans. Pode-se definir, por exemplo, que as portas 2,3,4,8 e 12 de um switch de 16 portas seja associadas à “VLAN1” enquanto as portas 1,5,6,7 e 15 pertencem à “VLAN2” e as portas 9,10,11,13,14 e 16 façam parte da “VLAN3”. Caso seja necessária alguma alteração ou movimentação de dispositivos deve-se reconfigurar as portas a fim de verificar se a nova porta faz parte da Vlan desejada. Pela facilidade de implementação e configuração é um dos métodos de agrupamento mais usado, sendo suportado por todos os fabricantes de equipamentos que suportam Vlans [7].

3.2.2 Agrupamento por Endereço Físico (MAC)

Outra forma de agrupamento de Vlans se faz através do endereço físico das interfaces de rede dos dispositivos (endereço MAC). Neste método, o administrador de redes associa um endereço MAC de um dispositivo a uma determinada Vlan no switch. Assim os dispositivos podem ser movidos para qualquer localização, dentro da organização, que continuarão a fazer parte da mesma rede virtual, sem qualquer reconfiguração posterior [2].

Talvez um dos maiores inconvenientes desta modalidade de agrupamento é o fato de que, antes de se colocar em operação, devem-se cadastrar todos os endereços MAC dos dispositivos que serão conectados no switch e associá-los a suas respectivas Vlans, o que, dependendo do tamanho da rede, pode dispender bastante tempo de trabalho. Outra limitação desta solução refere-se a impossibilidade de associar mais de uma Vlan para cada endereço MAC.

3.2.3 Agrupamento por Endereço IP

Nesta modalidade, os dispositivos podem ser agrupados através de seus endereços ou sub-redes IP. Desta forma pode-se atribuir uma Vlan a dispositivos com IP específico [7]. Por exemplo, os dispositivos com IP 172.16.0.10, 172.16.0.11 e 172.16.0.12 pertencem à "VLAN2".

Porém, deve-se tomar cuidado especial com a política de distribuição de endereços IP na rede. Tanto a especificação manual dos endereços nos computadores, quanto a fixação dos endereços de acordo como o endereço MAC nos servidores DHCP acarretam uma carga extra de trabalho para administração dos endereços que podem se esgotar e impossibilitar a conexão de novos dispositivos.

3.2.4 Agrupamento por Endereço IP Multicast

Quando um dispositivo ingressa em um grupo Multicast, através de uma confirmação de uma notificação previamente recebida, este passa a fazer parte de um grupo capaz de receber pacotes através de multicast. Os pacotes IP multicast são enviados a um endereço que representa este grupo e que pode ser definido dinamicamente.

Enquanto este dispositivo fizer parte deste grupo multicast, fará também parte de determinada Vlan através do agrupamento por endereços IP multicast. Esta característica temporária agrega uma grande capacidade de flexibilização a este tipo de agrupamento. Estas Vlans também podem transpor o limite da rede interna, estabelecendo conexões Wan por serem capazes de passarem pelos roteadores [2].

3.2.5 Agrupamento por Protocolos

Em redes onde são suportados protocolos diferentes (IP, IPX, NetBIOS, Apple Talk) este método pode ser usado para agrupar cada protocolo em uma Vlan diferente. Os comutadores verificam cada pacote para identificar a qual rede virtual o mesmo está associado por meio do tipo de protocolo usado. Apesar de se basear em endereçamento de 3º nível estes comutadores não realizam funções de roteamento, sendo restritamente usado para identificação e agrupamento das Vlans.

Um dos benefícios do uso deste tipo de Vlan é a flexibilidade na localização e mudança de estações sem necessidade de reconfiguração. Por outro lado existe perda de

performance dos comutadores que suportam este agrupamento pela necessidade de verificação dos endereços na terceira camada ao invés da primeira (endereço MAC).

3.2.6 Combinação de Agrupamentos

Pelo apresentado nos itens anteriores pode-se notar que cada tipo de agrupamento possui suas vantagens e desvantagens. Pensando em aumentar a autonomia dos administradores em organizar suas redes da forma que melhor se adapte as suas necessidades, atualmente muitos fabricantes têm oferecido equipamentos capazes de mesclar os agrupamentos permitindo um nível ainda maior de flexibilização e criando Vlans híbridas com pelo menos dois tipos de agrupamentos.

3.3 Configuração das VLANs

As Vlans podem ser configuradas de três formas diferentes a fim de possibilitar que os dispositivos se conectem a elas. São elas: Configuração manual (ou estática), automática (ou dinâmica) e semi-automática (ou semi-estática). Mais detalhes sobre cada uma delas serão apresentados a seguir.

3.3.1 Configuração Manual

Num procedimento de configuração manual de Vlan as configurações iniciais e todas as alterações posteriores de configuração são de responsabilidade do administrador. Esta modalidade proporciona um algo grau de controle e administração. Mas dependendo do tamanho de rede implantada, este grau de administração pode tornar-se impraticável por depender da interferência de um operador, sendo que uma das principais vantagens do uso de Vlans é justamente não necessitar de reconfigurações constantes.

3.3.2 Configuração Automática

Num método de configuração automática de Vlan os dispositivos são conectados e/ou desconectados automaticamente das redes virtuais por meio de critérios ou políticas previamente configuradas pelo administrador como por exemplo grupos de trabalho ou identificação do dispositivo ou usuário conectado.

Este tipo de configuração é bem suportado em qualquer tamanho de rede, mas é altamente recomendado para redes de grande porte por facilitar a administração e ser mais flexível.

3.3.3 Configuração Semiautomática

A modalidade de configuração semiautomática abrange particularidades das duas configurações citadas anteriormente. Uma Vlan ajustada de forma semiautomática permite que as configurações iniciais sejam definidas manualmente e as futuras reconfigurações e migrações de estações e dispositivos são realizados dinamicamente ou vice-versa.

3.4 Identificação de quadros (frames)

Em um processo de comunicação, quando o tráfego de rede atravessa os comutadores, estes devem ser capazes de identificar a quais Vlans os pacotes fazem parte. Esta identificação pode ser feita através do reconhecimento dos quadros que pode ser realizada pelos métodos implícito e explícito:

- **Método implícito:** ou marcação implícita (implicit tagging) caracteriza os quadros que não são rotulados. Os comutadores identificam a Vlan a que este quadro pertence através de informações contidas em seus cabeçalhos como por exemplo, a porta por onde o quadro chegou ou cruzando o endereço MAC com a tabela de associação das Vlans, para assim encaminhar os pacotes para o destino correto [5]. Neste método os dispositivos da rede não necessariamente precisam saber que existe Vlans pois o quadro permanece inalterado;
- **Método explícito:** ou marcação explícita (explicit tagging) ocorre quando um dispositivo de rede marca (tagg) o quadro com um identificador de Vlan acusando a qual rede virtual este quadro pertence. Neste método os dispositivos precisam saber da existência das Vlans, pois são inseridas informações referentes a esta identificação no cabeçalho do quadro, alterando seu tamanho, e caso um dispositivo que não suporte Vlan receba o quadro, este será descartado [11]. Os dispositivos na rede devem também possuir uma base de dados, igual para todos, com informações de identificação de cada Vlan e onde encontrar estas informações nos quadros. Os dispositivos adicionam, ou não, a tagg de Vlan dependendo se o dispositivo de destino possui suporte, ou não, ao protocolo de Vlan (IEEE 802.1Q).

3.4.1 Classificação de frames

A construção de quadros relacionados à Vlans são definidos pelas normas IEEE 802.3ac e IEEE 802.1Q e podem ser classificados como Untagged frames; Priority tagged frames e Tagged frames:

- **Untagged frames:** são frames ethernet comuns, sem qualquer marcação adicional;
- **Priority Tagged frames:** são frames que possuem a informação de classe de prioridade (IEEE 802.1p) porém sem nenhuma informação sobre identificação da Vlan. A tagg de prioridade possui 3 bits de tamanho e permite oito valores possíveis, podendo variar de zero a sete;
- **Tagged frames:** são frames que possuem a identificação da Vlan a que pertence no campo VID (Vlan Indentifier) de oito bits.

Os frames *Untagged* e *Priority Tagged* realizam a identificação das Vlans a que pertencem por meio da associação de portas, endereços MAC, protocolos entre outros. Já os frames *Tagged* não necessitam de tal associação pois, como explicado anteriormente, já possuem a identificação da Vlan inclusa no cabeçalho.

Na figura abaixo pode-se visualizar um frame ethernet comum, conforme definição da norma IEEE 802.3ac, e a localização onde é inserida a identificação de Vlan (Tagg).

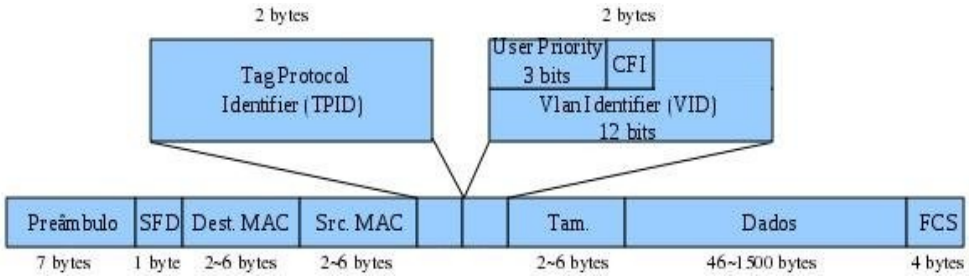

Figura 4: Quadro Ethernet e Tagg Vlan

A inserção das taggs Vlan caracterizam-se pela adição de dois campos de dois bytes, posicionados após o campo de endereço MAC de origem, com o primeiro denominado *Tagg Protocol Identifier* (TPID) que identifica um frame com marcação (normalmente com o valor 0x8100) e o segundo campo chamado *Tagg Controll Information* (TCI) que é subdividido em três campos identificados como *User Priority* (3 bits de tamanho) que define a prioridade do frame, o campo *CFI* (Canonical Form Indicator - 1 bit) que foi projetado para uso em redes Token Ring e o campo *VID* (Vlan Identifier – 12 bits) que é o campo reservado para identificação de Vlans [7].

Se o valor do campo *VID* for nulo (0x000) significa que o campo não possui informação de identificação e o TCI possui apenas informação de prioridade. Se o valor for igual a "1" (0x001) significa que o quadro é um Vlan-Tagged frame. O valor de VID setado como FFF (0xFFF) é reservado e não pode ser usado para identificação e configuração de Vlans.

O quadro padrão Ethernet, após a inclusão da tagg Vlan sofre um acréscimo em seu tamanho máximo, passando de 1518 para 1522 bytes e precisa ter o FCS (Frame Check Sequence) recalculado para não ser identificado como pacote corrompido por outros dispositivos de rede, e estes devem também possuir suporte para identificação de quadros Vlan, do contrário os pacotes serão descartados [8].

3.5 VLAN Trunking

O conceito de Vlan Trunking é definido pela norma IEEE 802.1ad e caracteriza-se por ser capaz de transportar tráfego de mais de uma Vlan no mesmo circuito. Conforme Barros [12] "em uma rede comutada um tronco é um link ponto-a-ponto que suporta várias Vlans." A identificação das Vlans em um enlace configurado no modo Trunk (tronco) é feita através dos métodos de marcação de quadros (Vlan-tagging).

Neste modelo de funcionamento todos os dispositivos interconectados devem ter suporte a identificação de membros e dos formatos de quadros de Vlans (Vlan-aware) [12]. Dispositivos de rede que não suportem o reconhecimento de Vlans não propagarão tráfego deste tipo descartando os quadros, interrompendo e/ou impedindo a comunicação dos dispositivos interligados por este aparelho.

As portas dos dispositivos de rede podem ser configuradas, além do modo Tronco, no modo Access (acesso) que, ao contrário do trunking, restringe o enlace a trafegar pacotes de uma única Vlan por meio de configuração prévia [14]. Portas configuradas em modo Acesso também não reconhecem quadros com marcação IEEE 802.1Q e descartam todo conteúdo deste tipo que alí chegar.

A comunicação entre dois dispositivos com suporte à Vlan também só efetivamente ocorre quando as portas que os conectam estiverem configuradas de maneira adequada. Ao se

conectar dois switches que funcionam com várias Vlans por exemplo ambas as portas devem estar configuradas como Trunk ou a conexão não será estabelecida. Já a porta de um switch que se conecta a uma estação final (computador pessoal) recomenda-se que seja configurada como Acesso para que o computador se conecte à rede sem a necessidade de configurações específicas.

Na figura abaixo podemos visualizar o funcionamento de uma rede com Vlans que utilizam o conceito de Trunking para interligar os switches que possuem computadores membros de diferentes redes virtuais. Os enlaces que possuem computadores ligados em uma de suas extremidades são configurados no modo Acesso.

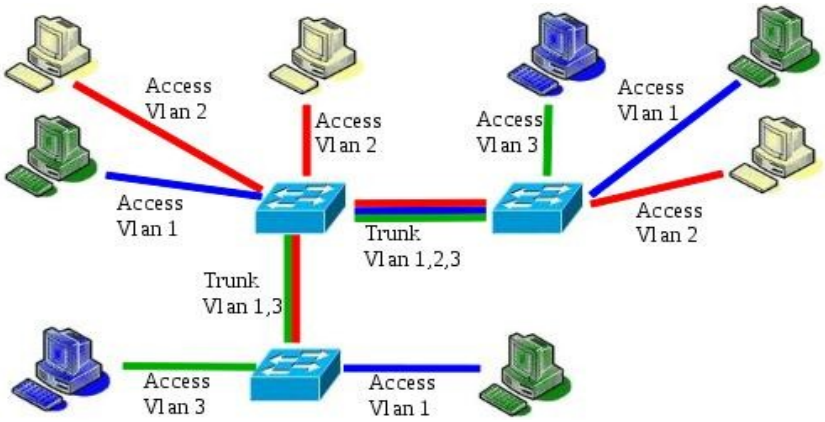

Figura 5: Disposição dos enlaces Trunking e Access

Em switches da fabricante Cisco Systems o administrador de redes pode também fazer uso do protocolo VTP (Vlan Trunking Protocol) a fim de simplificar a configuração das Vlans em uma rede com diversos switches. O protocolo VTP faz a propagação das configurações realizadas em um switch para os demais que suportem o mesmo protocolo, em média, a cada 5 minutos [15]. No caso de se realizar a adição de uma nova Vlan em uma rede com dez switches, o administrador de redes deve configurar, um a um, os aparelhos que irão aceitar este tráfego e por quais portas este tráfego passará. Com o uso do protocolo VTP o administrador de redes necessita configurar um único switch e as configurações ou alterações serão propagadas aos outros switches da rede. Para que o protocolo funcione é necessário configurar todos os dispositivos para operarem como membros de um domínio VTP.

Os dispositivos que têm suporte ao uso do protocolo VTP podem trabalhar em três modos de configuração:

- **VTP Server:** quando o switch está no modo *VTP Server*, as configurações de trunking (número e nomes das Vlans) são armazenadas na memória não volátil do aparelho. Por padrão todos os switches vêm configurados de fábrica para operar no modo VTP Server. Qualquer alteração feita nas configurações será propagada para todo o domínio VTP;
- **VTP Client:** os switches configurados como *VTP Client* somente recebem e aplicam as alterações realizadas no *VTP Server*. As configurações também são armazenadas na memória não volátil mas não é possível efetuar alterações através dos aparelhos configurados neste modo. Normalmente os dispositivos clientes são conectados diretamente aos servidores através de portas trunk.
- **VTP Transparent:** no modo *VTP Transparent* o switch não participa do domínio VTP, não recebendo as configurações do *VTP Server*, mas é capaz de encaminhar atualizações VTP. Em um dispositivo que funciona no modo transparente é possível

efetuar configurações localmente sem interferir na configuração de outros switches, sejam estes membros de um domínio VTP ou não.

Quando as configurações do *VTP Server* são alteradas, um novo número de revisão é criado e, após completado o prazo de cinco minutos, anunciado a todos os membros do domínio VTP. Os clientes então solicitam, recebem e aplicam a nova configuração automaticamente, sem intervenção do administrador [16].

3.6 Roteamento entre Vlans

Como já foi apresentado anteriormente, as Vlans são comumente destinadas a segmentação de redes para as mais variadas aplicações e por diversos motivos. Porém, em muitos casos estas Vlans têm a necessidade de se comunicar, e isto só é possível quando são usados dispositivos com funções de roteamento.

Existem atualmente três formas de roteamento entre Vlans: através de múltiplos enlaces, através de Enlace único com Trunking e por dispositivo de comutação com processador de rotas interno (switch de camada 3). Nos sub-tópicos a seguir os três modelos serão apresentados com mais detalhes.

3.6.1 Roteamento através de múltiplos enlaces

Neste método de roteamento um enlace de cada Vlan deve estar conectado às portas do roteador. Este modelo é muito utilizado em roteadores que não possuem suporte a tratamento de frames no padrão IEEE 802.1Q e onde os links são obrigatoriamente configurados no modo enlace.

Esta solução é bem suportada em redes de pequeno porte mas torna-se inviável para estruturas maiores pois demandaria roteadores de grande capacidade, tanto na quantidade de portas quanto na capacidade de processamento, para interligar todas as Vlans.

Na figura abaixo é apresentado um exemplo de uso de um roteador com várias portas para interconectar cada uma das Vlans de uma determinada estrutura física.

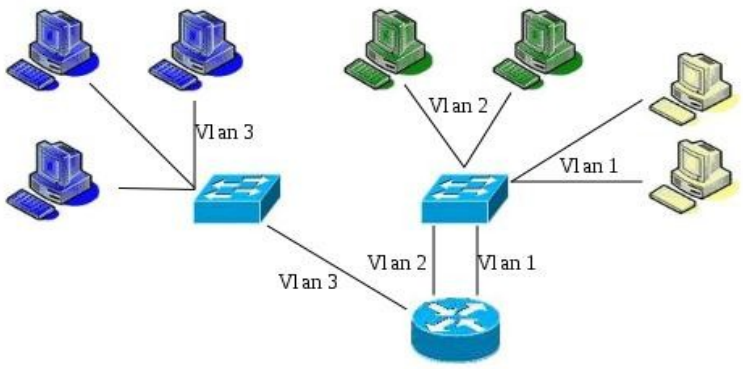

Figura 6: Roteamento por múltiplos enlaces

3.6.2 Roteamento através de enlace único com Trunking

Este conceito, como o o próprio nome já diz, consiste em utilizar a tecnologia de

trunking para concentrar todas, ou a maior quantidade possível, de Vlans em uma mesma conexão física do switch ao roteador [11]. Para que isto seja possível o roteador precisa necessariamente possuir suporte à Vlans.

Neste tipo de configuração a porta do switch e do roteador que se comunicam são configuradas no modo trunking. No roteador são criadas interfaces virtuais com as configurações de rede de cada Vlan. Quando existe a comunicação entre dispositivos de Vlans diferentes, os frames atravessam este enlace até o roteador que realiza o encaminhamento deste e envia de volta pelo mesmo caminho, agora pertencendo a Vlan do dispositivo de destino.

Na figura abaixo é apresentado um exemplo de roteamento entre Vlans utilizando um único caminho em modo Trunking entre o switch e o roteador.

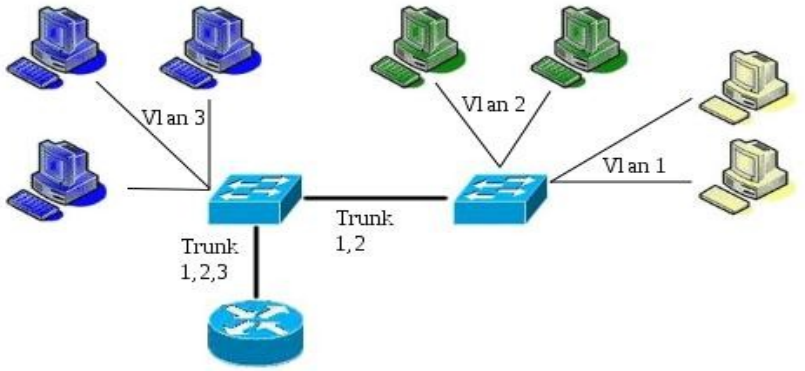

Figura 7: Roteamento por enlace único com Trunking

Esta solução é a mais econômica, prática e rápida de ser implementada em uma rede com Vlans pois não exige compra de novos equipamentos e pode ser implementada sem a necessidade de alterar a estrutura física de rede.

3.6.3 Roteamento por comutador com processador de rotas interno (switch de camada 3)

Este método de roteamento carateriza-se pelo uso de comutadores com propriedades de manipulação de dados da terceira camada OSI (Transporte), mais conhecidos como switches de camada três (ou de terceira camada). Este comutador possui a grande vantagem de somar todas as funções de comutação e roteamento em um único aparelho ganhando-se em espaço físico e velocidade de transmissão dos dados, visto que estes atravessam um único aparelho e a velocidade de transmissão interna entre os módulos de comutação e roteamento é muito maior se comparada com a velocidade de um enlace em par trançado.

Estes switches de terceira camada têm a capacidade de criação de interfaces de rede virtuais, chamadas SVI's (Switch Virtual Interface) que são associadas a cada Vlan da rede [14]. Estas SVI's encaminham os frames das Vlans para o roteador interno que se encarrega de realizar a interconexão entre as diferentes Vlans.

Na figura a seguir é mostrado um cenário onde se utiliza um comutador de camada três para implementar o roteamento entre as Vlans de uma determinada rede física segmentada por Vlans.

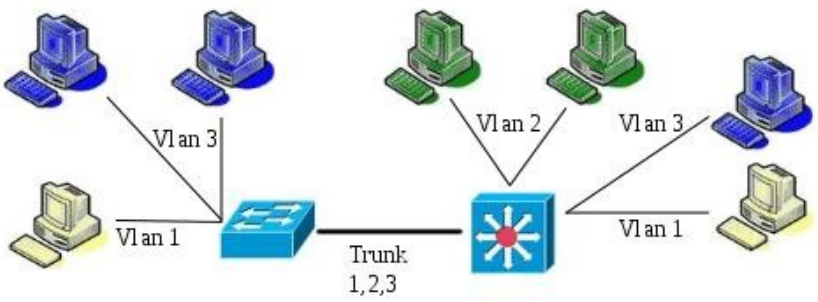

Figura 8: Roteamento por switch de terceira camada

Este modelo de roteamento é extremamente eficiente, sendo a melhor entre as três soluções apresentadas. Por outro lado, os custos de aquisição de equipamentos de comutação de camada três ainda são um pouco elevados, tornando-o viável apenas em estruturas grandes onde o uso de roteamento por enlace único com trunking deixar de ser vantajoso.

3.7 Spanning Tree

Atualmente, para garantir a disponibilidade de acesso nas redes locais, têm-se optado por investir em caminhos redundantes de acesso. Esta redundância pode ser alcançada interligando-se os switches da rede interna em forma de anel, onde o último switch se conecta ao primeiro. Porém, esta solução pode literalmente parar a rede, visto que existiria mais de um caminho para se alcançar o mesmo destino, o que ocasionaria loops até a completa exaustão do enlace.

Para evitar os problemas ocasionados pela redundância de acessos foi desenvolvido o protocolo STP (Spanning Tree Protocol) definido pela norma IEEE 802.1d que garante que haja somente um caminho válido para cada destino. Souza [17] diz que " o objetivo do STP é criar uma topologia redundante e, ao mesmo tempo, livre de loops". Os enlaces classificados como redundantes são bloqueados (estado *blocking)*, de forma lógica, sem que seja necessário qualquer intervenção física na estrutura de rede. O enlace bloqueado fica em modo de espera (stand-by) e será imediatamente restabelecido (estado *forwarding)* caso haja alguma interrupção no link primário, garantindo a redundância da rede.

Na figura abaixo podemos observar uma rede redundante usando-se o princípio de Spanning Tree. Note que, em um dos enlaces que interligam os switches, o cabeamento continua conectado, mas o protocolo STP se encarrega de efetuar o bloqueio lógico do caminho para evitar que a rede entre em loop.

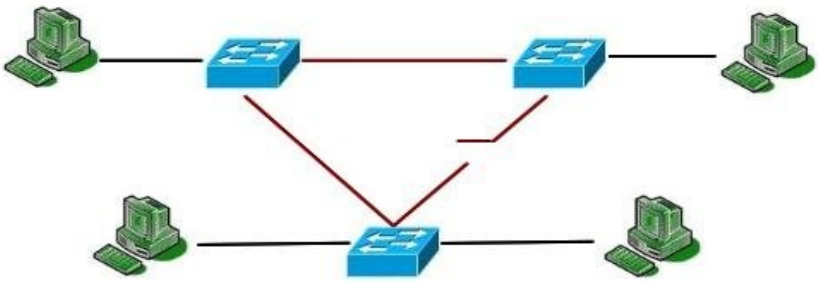

Figura 9: Lan com Spanning Tree

A topologia do protocolo STP é definida em forma de árvore, onde um switch é definido como raiz ou root (root switch) e o restante dos switches como "não-root" (non-root

switch), sendo que o switch raiz define quais enlaces serão bloqueados e quais ficarão ativos. Para que isto seja possível todos os dispositivos devem suportar o protocolo IEEE 802.1d e tê-lo ativado.

Para que uma rede esteja efetivamente livre de loops o protocolo STP deve concluir três etapas:

• **Definição do Switch raiz ou root:** Nesta etapa, ao serem ligados, os switches trocam entre si BPDU's (Bridge Protocol Data Unit) com o *Bridge ID* do switch, que consiste em dois subcampos chamados *Bridge Priority* e *MAC Address* para definir qual será o switch raiz da rede [17]. Todos os switches que suportam o protocolo STP vêm, por padrão, com a prioridade setada como 32768, mas esta pode ser alterada caso o administrador queira forçar a eleição de um dispositivo como raiz. Caso o número de identificação da prioridade seja igual em todos os dispositivos será então eleito o menor endereço MAC. No início da negociação todos switches se autodenominam como sendo raiz, mas conforme negociação ocorre, estes devolvem mensagens aceitando a eleição de um dispositivo com *BID* menor. Na figura abaixo podemos verificar que a eleição do "switch 1" como root foi devido ao seu endereço MAC ser menor que dos outros aparelhos.

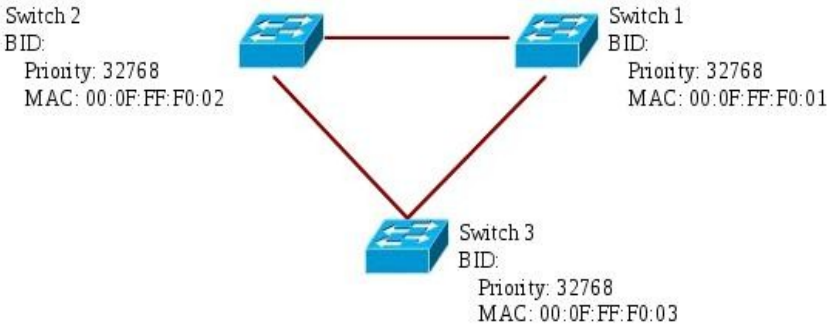

Figura 10: Eleição do switch raiz

• **Definição das portas principais:** Os switches classificados como "não-root" devem então definir sua porta raiz. A porta designada como raiz do switch não-root é a que tiver o menor custo acumulado do enlace para alcançar o switch raiz [18]. Este processo ocorre logo após a definição do switch raiz e é realizado por meio de trocas de BPDU's. Os custos podem ser customizados para forçar a eleição de determinado caminho ou pode-se utilizar os valores definidos por padrão. Na tabela abaixo são apresentados os custos de alguns enlaces conforme sua velocidade de transmissão:

Velocidade do Link	Custo do enlace
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

Tabela 1: Custos dos enlaces

• **Definição das portas designadas:** A definição das portas designadas nos switches também ocorre pelo cálculo do menor custo entre o caminho raiz (root-path cost) até o switch raiz após a definição das portas raiz [17]. As portas do switch raiz, por terem normalmente os menores custos, também são definidas como portas designadas. Caso haja igualdade de custos na comparação de algum segmento, o desempate ocorre pela comparação do menor endereço MAC do BPDU. A porta que obtiver o maior custo da rede torna-se uma porta não-designada (non-designated port), entrando no estado blocking. Na figura abaixo podemos visualizar a eleição das portas designadas. Note que uma porta do switch 3 foi bloqueada por ter o maior custo observado.

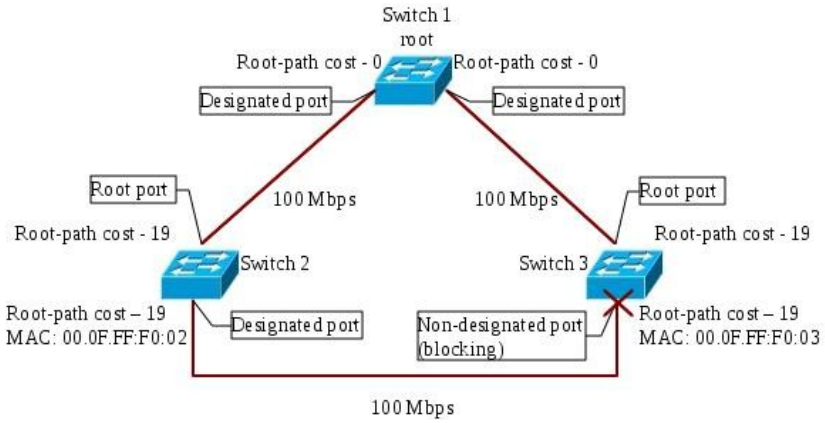

Figura 11: Definição das portas designadas

Desde o processo de inicialização de um switch e durante sua operação suas portas podem ser habilitadas, ou não, a trafegar dados de acordo com a topologia da rede identificada pelos dispositivos ou por mudanças causadas por falhas ou intervenção técnica. Sendo assim podem ser identificados quatro estados: bloqueado (blocking), escutando (listening), aprendendo (learning) e encaminhando (forwarding). Estes estados são cruciais para o funcionamento do spanning tree pois desta forma loops na rede podem ser desativados e ativados quase que instantaneamente.

• **Bloqueado (blocking):** Ao inicializar um dispositivo todas as portas são definidas no estado blocking para evitar o fechamento de supostos loops na rede. Neste modo não é possível transmitir dados nem armazenar informações de endereços. Somente a troca de BPDU's entre os aparelhos é possível.

• **Escutando (listening):** Neste modo o dispositivo já recebe dados mas não pode retransmití-los adiante. Somente BPDU's são recebidos e enviados. Neste estágio é onde ocorre a definição dos switches raiz, portas raiz e designadas e quando são definidas as portas que permanecerão bloqueadas.

• **Aprendendo (learning):** No estado learning, o dispositivo identifica e grava, em sua tabela, novos endereços MAC na rede. Neste estágio que é desenhada a árvore da rede. Ainda não é possível trafegar dados sendo este o nível que precede o estado em que o encaminhamento de frames é permitido.

• **Encaminhando (forwarding):** Nesta etapa o tráfego de BPDU's e principalmente dados é liberado e os dispositivos de rede podem se comunicar livremente. Antes porém de designar a porta como apta a forwarding o protocolo STP se certifica de que não haja caminhos redundantes ou pontos de loop na rede.

Com todo este procedimento necessário, é natural que o processo de inicialização de uma rede que funcione com Spanning Tree seja razoavelmente demorado, durando entre trinta e cinquenta segundos. Porém, para tornar este processo de inicialização mais ágil, o IEEE aperfeiçoou o protocolo STP criando o Protocolo Spanning Tree Rápido (Rapid Spanning Tree Protocol) definido pela norma IEEE 802.1w. O RSTP caracteriza-se principalmente pelo seu tempo de inicialização, que pode variar de dois a dez segundos. Dispositivos que suportam os protocolos IEEE 802.1d e IEEE 802.1w podem funcionar com os dois em paralelo, isto é, em um switch podem haver links ativos com STP e outros com RSTP, mas nunca os dois ativos no mesmo enlace.

3.7.1 Per Vlan Spanning Tree Protocol (PVSTP)

A fim de tornar o conceito de Vlans ainda mais flexível desenvolveu-se uma forma de conciliar a possibilidade de se obter uma rede redundante aliado ao poder de segmentação de redes virtuais adicionando a vantagem de balanceamento de tráfego pelos enlaces. Esta solução foi denominada Per-Vlan Spanning Tree Protocol, sendo este um protocolo proprietário da Cisco.

O protocolo PVSTP atribui uma instância STP para cada Vlan criada tornando o gerenciamento da árvore STP independente em cada rede virtual. Portanto cada Vlan pode usar enlaces distintos o que proporciona ainda o balanceamento de tráfego de dados pelos links redundantes.

Por meio deste protocolo todos os enlaces são aproveitados sendo que cada Vlan pode percorrer um caminho diferente pelos switches para alcançar seu destino [17], isto é, uma porta que está marcada com estado *blocking* para uma Vlan pode estar no estado *forward* para uma segunda Vlan e assim por diante.

A separação das rotas de cada Vlan com redundância pode ser conseguida através da eleição de prioridades para as Vlans em cada enlace tronco [14]. Por padrão todas as portas vêm configuradas com a prioridade 128 para todas as portas, mas esta prioridade pode ser alterada de acordo com as rotas que se deseja estabelecer para cada Vlan. É possível, por exemplo, estabelecer que a Vlan 1 e a Vlan 2 tenham prioridade 12 e 128 respectivamente em um enlace “A” e prioridades 96 e 24 respectivamente no enlace “B”. Desta forma, os pacotes da Vlan 1 terão preferência de tráfego no enlace “A” e a Vlan 2 terá preferência no enlace “B”.

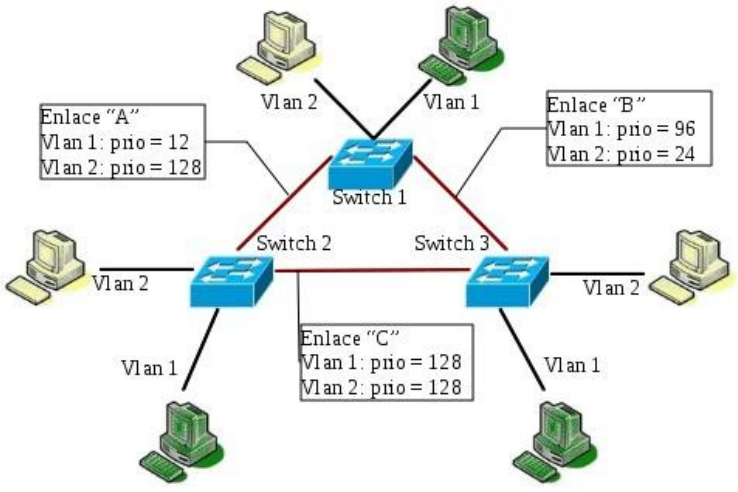

Figura 12: Redundância e balanceamento de tráfego com PVSTP

Na figura acima pode-se visualizar um exemplo de uso do protocolo PVSTP para obter-se redundância e melhor aproveitamento da estrutura de rede. Note que nenhum enlace está definitivamente bloqueado. Os enlaces “A” e “B” tem prioridades distintas para as Vlans 1 e 2, sendo que, na ocorrência de falha em um destes links, o outro assume imediatamente compartilhando as duas Vlans. Já o Enlace “C” possui prioridade igual para as duas Vlans para suportar o tráfego de ambas ao mesmo tempo.

3.7.2 Multiple Spanning Tree Protocol (MSTP)

Um outro protocolo disponível para implementação de Vlans com Spanning Tree é o Multiple Spanning Tree Protocol (MSTP) regulamentado pela Norma IEEE 802.1s. Neste protocolo existe a possibilidade de se criar algumas instâncias MST (normalmente até 65) que podem suportar uma quantidade realmente grande de Vlans [19]. Desta forma podem ser acumular em uma instância o tráfego de cem Vlans para percorrer um determinado enlace e agrupar em uma segunda instância outras cinquenta Vlans para trafegar por um segundo enlace por onde a primeira instância teria uma prioridade menor e vice-versa.

O protocolo MSTP é executado sobre o RSTP, tornando seu uso obrigatório, e utiliza um sistema de mensagens BPDU diferenciado em relação ao original permitindo que sejam transportadas as informações de instâncias necessárias ao protocolo. Cada instância propaga os BPDU's com informações sobre as Vlans pertencentes a esta [14].

O protocolo MSTP pode oferecer uma maior escalabilidade, se comparado ao PVSTP, quando se utiliza o conceito de divisão em regiões. Neste conceito uma região pode possuir várias instâncias de Vlans e podem haver diferentes regiões em uma rede local interligadas. Para isto é necessário que exista uma instância mestre chamada Internal Spanning Tree (IST), ou instância zero, que transmite somente BPDU's e uma ou mais regiões MST por onde são transmitidos os MST BPDU's e onde as instâncias são criadas.

Na figura abaixo é apresentado um exemplo de uso de MSTP com a aplicação do conceito de regiões MST.

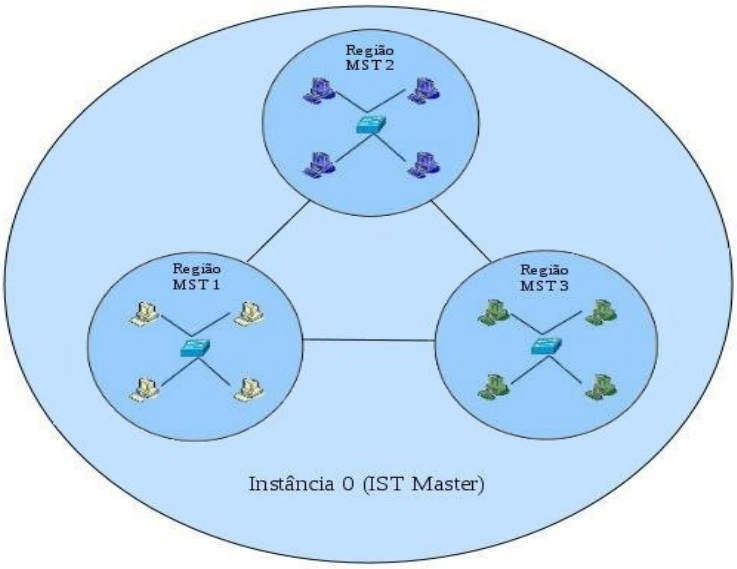

Figura 13: Regiões MSTP

4 Análise comparativa

Existem atualmente diversas tecnologias e opções de implementação de Vlans disponíveis nos dispositivos de rede mais avançados. Cada solução possui suas características e diferentes empregabilidades que podem variar conforme o cenário da estrutura de rede apresentado. Avaliar todas estas soluções poderia tornar este trabalho extremamente extenso. Para simplificar e tornar o assunto bem direto optou-se por dividir os temas da análise em subtítulos avaliando então as soluções mais vantajosas levando em consideração o foco da discussão.

Nos itens dispostos a seguir realizar-se-á uma análise das melhores soluções de implementação de Vlans sob o ponto de vista da segurança, gerenciamento e qualidade do serviço.

4.1 Segurança

Um dos principais benefícios da utilização de Vlans para segmentação de redes é a segurança, visto que esta proporciona uma separação lógica do tráfego de uma rede virtual composta por servidores, por exemplo, da rede virtual dos usuários de uma corporação. Porém, o uso de algumas soluções complementares pode reforçar ainda mais a segurança de uma rede composta por Vlans.

Um aspecto necessário e muito sensível quando se trata de Vlans é o roteamento de tráfego entre as diferentes redes virtuais. Em qualquer implementação de Vlan faz-se necessário interligar as redes com roteadores, e é desejável que haja garantias de que nenhuma delas seja acessada por membros de outras Vlans, exceto quando necessário e autorizado. O uso de roteadores com o auxílio de ferramentas de filtragem de pacotes (firewall) são muito eficientes na função de alcançar este nível de segurança.

O método de roteamento com Switch de camada 3 é o mais vantajoso em termos de segurança, ainda mais se este dispuser de firewall interno reunindo assim, em um só aparelho, as funções de comutação, roteamento e filtragem de pacotes tornando-o muito mais rápido se comparado ao uso conjunto de um roteador com um switch comum (camada 2). No entanto o custo de aquisição deste tipo de switch ainda é muito elevado e nem todas organizações têm condições de equipar suas redes com esta solução.

Uma opção mais viável, porém não tão eficiente, é o uso do método de roteamento de enlace único com Trunking, onde um comutador de camada 2 e suporte à Vlan conecta todas as redes virtuais a um roteador por meio de um enlace em modo tronco. Para simplificar a estrutura e implementar a segurança desejada pode-se substituir o roteador por um computador configurado para realizar as funções de roteamento e filtragem de pacotes. Este computador precisa ter boa capacidade de processamento e interfaces de rede com velocidades compatíveis com o tráfego dos enlaces, visto que o tráfego de todas as Vlans passará por estas interfaces.

No entanto nada impede que se faça o uso conjunto das duas soluções em uma mesma estrutura de rede. Os comutadores de camada 3 podem ser instalados nos enlaces que constituem o tronco da rede (Core), onde o tráfego de todas as Vlans se concentra e onde se localizam os servidores que proverão os acessos. Saindo do tronco e dirigindo-se a periferia da estrutura, composta basicamente por estações de trabalho e periféricos não existe mais a necessidade de usar equipamentos tão sofisticados e pode-se usar o roteamento de enlace

único com trunking. Mas em todos os casos, é imprescindível o uso de um bom firewall para evitar riscos de segurança na comunicação entre as Vlans.

Outra questão importante a se considerar com relação a segurança é o tipo de configuração das Vlans. Em uma Vlan configurada de forma estática existe o risco, por menor que seja, de um dispositivo ser conectado a uma rede virtual errada, seja involuntariamente, por negligência ou propositalmente fazendo com que este passe a fazer parte de outra Vlan onde pode ter acesso a informações sigilosas da organização. Não se pode negar porém que em redes pequenas, onde exista um bom controle visual da estrutura, uma Vlan estática é vantajosa pois não exige muito tempo e planejamento para configurar e implantar, mas em estruturas maiores, além de dificultar o gerenciamento, existe o risco de mudanças indevidas de cabeamento, colocando em risco a segurança da rede e tornando-a vulnerável a eventuais ataques.

Um método mais adequado de configuração de Vlans seria o automático ou semiautomático. Tanto no modo automático, como no semiautomático, a inserção de um dispositivo é toda baseada em regras previamente configuradas, sendo que no modo semiautomático parte desta configuração inicial ou posterior pode ser feita manualmente, e onde quer que o equipamento seja conectado, este sempre pertencerá a mesma Vlan, a menos que haja alguma alteração nas regras ou configurações pelo administrador da rede. Assim não há riscos de segurança por mudanças inadvertidas de cabeamento ou dispositivos como no método de configuração manual. Estes modos, no entanto, exigem um maior conhecimento dos administradores de rede para realizar todas as configurações necessárias de modo a não permitir a entrada de dispositivos não conhecidos em uma Vlan restrita.

4.2 Gerenciamento do serviço

Diversos fatores podem influenciar na capacidade e facilidade do gerenciamento de uma estrutura de Vlans, tanto para melhor quanto para pior. É preciso analisar com cautela e atenção todas as opções disponíveis antes da implementação do serviço para evitar problemas como a lentidão e indisponibilidade dos serviços oferecidos ou da rede como um todo motivados por carga excessiva de ações de gerenciamento sobre o administrador de redes.

Uma das ações que podem facilitar o gerenciamento das Vlans é a escolha dos tipos de agrupamento destas. Os agrupamentos por endereços MAC ou por porta do switch são bastante simples, rápidos de serem aplicados e, principalmente, gerenciados quando aplicados em redes pequenas e onde se conhece a quantidade exata de dispositivos conectados e os novos que serão adicionados a esta.

Mas conforme as proporções da estrutura aumentam estes tipos de agrupamento podem tornar-se inviáveis em relação ao gerenciamento devido, dentre outros fatores, ao tamanho que as tabelas de atribuição das Vlans nos dispositivos de rede irão adquirir e a dificuldade nas ações de alteração de local dos inúmeros dispositivos, substituições de interfaces de rede ou adição/remoção de equipamentos que forem solicitados. Nestes casos torna-se mais vantajoso o uso dos métodos de agrupamento mais refinados, como por IP, Protocolo ou Multicast (estes dois últimos dependendo da finalidade) mas, principalmente, a combinação de alguns dentre todos os modos apresentados desde que o resultado desta combinação diminua o máximo possível a intervenção do administrador de redes a cada modificação ou adição dos equipamentos e periféricos dispersos na rede mas mantendo o nível do serviço prestado.

Os modos de agrupamentos configurados isoladamente podem resolver

momentaneamente algumas necessidades, mas com o tempo podem tornar-se insuficientes na tarefa de atribuição de Vlans a novos equipamentos conectados. Os melhores resultados são alcançados quando são usadas combinações de agrupamentos. Sua configuração pode ser bastante complexa e criteriosa mas, quando bem configurados, possibilitam atender uma grande diversidade de situações onde os equipamentos se conectam à rede sem que, em alguma ocasião, seja necessária a intervenção do administrador de redes para validar conexões ou modificar regras de agrupamento para possibilitar o ingresso de um novo dispositivo à rede.

Os modos de configuração das Vlans além da segurança, como apresentado no tópico anterior, também podem simplificar o gerenciamento de uma rede de Vlans. Novamente os modos automático e semiautomático tornam-se mais apropriados para uso em redes de proporções média e grande também por diminuir a interação do administrador de redes no momento em que os equipamentos são conectados, removidos ou tiverem seu ponto de conexão alterado. O modo estático não deixa de ser uma opção, mas seu uso é vantajoso apenas em redes menores pela rapidez e facilidade de implantação e gerenciamento.

Outro assunto importante a se tratar, em relação a gerenciamento de Vlans é a gestão das rotas e do tráfego pela estrutura física de rede. As soluções avançadas de Spanning Tree (PVSTP e MSTP) são ótimas opções de gerenciamento de tráfego dividindo o fluxo de dados por enlaces redundantes e com mudança automática de rotas quando se detecta a interrupção de algum caminho.

Em relação a estas duas tecnologias de spanning tree o MSTP pode oferecer vantagens no gerenciamento de redes compostas por uma quantidade grande de Vlans se comparado ao PVSTP. Por ter a possibilidade de divisão de regiões onde podem ser agrupadas uma infinidade de Vlans, O MSTP proporciona uma melhor percepção visual da estrutura de Vlans o que agiliza a execução de ações de gerenciamento.

O protocolo PVSTP também é simples de gerenciar apesar de suportar uma quantidade menor de Vlans, sendo mais recomendado para redes com uma quantidade limitada de redes virtuais. Porém, por ser proprietário da Cisco, seu uso obviamente só será possível em uma rede que contenha comutadores deste fabricante, ao contrário do MSTP que é um protocolo aberto e pode estar disponível em qualquer equipamento que possua suporte a Vlan

4.3 Qualidade do serviço

A qualidade do serviço de Vlans pode ser considerado como sendo o ponto mais perceptível aos usuários da rede, visto que, melhorando a qualidade da rede existe uma melhora no tempo de resposta e menor risco de indisponibilidade dos sistemas disponibilizados. A implantação de Vlans, por si só, já tende a melhorar o tráfego de dados isolando a propagação de broadcasts e multicasts na rede virtual a qual este foi gerado.

Avaliando-se este quesito a implantação de Vlans utilizando-se as tecnologias de Spanning Tree possibilitam um grande salto na velocidade da rede de modo geral. Uma rede comum, estruturada em forma de árvore, sofre um afunilamento de tráfego em sua raiz, o que restringe a velocidade dos clientes localizados na periferia. Quando se utiliza o STP a estrutura física passa a ter a forma de anel, mas o protocolo trata de garantir que haja apenas um caminho ativo para se alcançar determinado destino dividindo o tráfego das Vlans por enlaces diferentes e ainda oferece a redundância de rotas, alterando o caminho a ser percorrido por determinada Vlan caso algum de seus enlaces físicos seja interrompido.

Dentre as tecnologias STP estudadas tanto o PVSTP quanto o MSTP possibilitam que se alcance este cenário de redundância e balanceamento do tráfego de rede. A vantagem do protocolo MSTP em relação ao PVSTP é a melhor performance do hardware no gerenciamento de várias Vlans ao mesmo tempo por possibilitar o agrupamento de várias redes virtuais em um única instância MST e o fato de ser um padrão aberto e disponível em qualquer equipamento que suporte Vlans, ao passo que o protocolo PVSTP, como já mencionado anteriormente, é proprietário da empresa Cisco Systems.

O roteamento entre Vlans também pode ser uma opção a fim de melhorar o serviço disponibilizado. Em uma boa estrutura física para implantação de Vlans é necessário que existam comutadores, roteadores e firewalls para interligar as redes e reter tráfego não autorizado. Considerando que cada equipamento seja conectado a outro através de cabeamento padrão de rede (metálico par-trançado) pode se concluir que haverá um certo atraso (delay) no trânsito dos pacotes pela rede. Quanto maior for a quantidade de Vlans, maior a necessidade destes tipos de equipamentos para interligá-las e maior será a taxa de atraso do tráfego de rede.

Os roteadores de camada três possibilitam que em um único aparelho sejam realizadas estas três etapas (comutação, roteamento e filtragem de pacotes) com a vantagem de que a velocidade de transmissão dos dados é equivalente ao barramento interno do equipamento, que é inúmeras vezes maior do que a velocidade de um cabo de rede, além de que estes equipamentos são construídos especificamente para este fim e seu software é otimizado para obter o melhor desempenho sob qualquer condição. Apesar de serem caros, se comparados a outras soluções usando comutadores de camada 2, seu benefício é facilmente justificável pelo desempenho alcançado em redes com grande fluxo de tráfego.

5 Conclusão

Ao final deste artigo pode-se concluir que, dentre as inúmeras tecnologias desenvolvidas para prover soluções de segmentação de redes com Vlans, não existe um modelo a ser seguido ou um manual de melhores práticas para a obtenção de uma estrutura de Vlans eficiente, segura e prática. Cada cenário pode resultar no uso de diferentes tecnologias que focam a solução de determinadas necessidades. O ponto mais importante de um projeto de implantação de Vlans é uma boa análise das tecnologias disponíveis capazes de suprir as necessidades da rede da organização.

Porém, algumas vantagens alcançadas com a implantação de Vlans em uma rede são indiscutíveis, dentre elas, a melhoria significativa da trafegabilidade de dados na rede de modo geral devido, principalmente, a contenção de pacotes de difusão, problema crescente nas médias e grandes redes corporativas, o avanço nas condições gerais de segurança da rede impedindo acessos não autorizados e delimitando áreas que demandam maior ou menor atenção em relação a segurança e a reutilização de equipamentos existentes na estrutura atual, proporcionando economia de custos e obtenção de resultados. Estas características podem ser ainda mais aperfeiçoadas se utilizadas determinadas tecnologias para apurar a própria segurança, o gerenciamento e a qualidade de uma estrutura de Vlans.

Para dar sequência na linha de estudos poderia-se aprofundar a avaliação da qualidade do serviço estudando soluções para controle de tráfego com Vlans a fim de priorizar determinados tipos de serviços essenciais e também avaliar as formas de roteamento e filtragem de pacotes para apurar a segurança e a conectividade das redes virtuais.

6 Referências Bibliográficas

[1] Prado, Fernando Ferreira do. **Virtual LAN's .** Disponível em: http://www.gta.ufrj.br/grad/98_2/ fernando/fernando.html . Acesso em: 02 ago. 2009.

[2] Passmore, D. Freeman, J. (1997)**. The Virtual LAN Technology Report**. Disponível em: http://www.3com.com/other/pdfs/solutions/en_US/20037401.pdf. Acesso em: 02 de ago. 2009.

[3] Dell Corp. (2004). **VLAN-Based Network Segmentation**. Disponível em: http://www.dell.com/ downloads/global/products/pwcnt/en/app_note_8.pdf . Acesso em: 8 ago. 2009.

[4] Both, José Luiz. **Excerto da Pré-norma IEEE 802.1Q**. Disponível em: http://www.pop-rs.rnp.br/~berthold/etcom/redes2-2000/trabalhos/802_1q.htm . Acesso em 22 jul. 2009.

[5] Moraes, Igor Monteiro. **VLANs - Redes Locais Virtuais**. Disponível em: http://www.gta.ufrj.br /grad/02_2/vlans/. Acesso em 22 jul. 2009.

[6] Cisco Systems Inc. **Conhecimentos Básicos de Redes (CCNA 1)**. 2008.

[7] Coelho, Paulo. **Redes Locais Virtuais – Vlans.** Disponível em: http://www.estv.ipv.pt/ PaginasPessoais/pcoelho/rc/Material%20RC/vlans.pdf . Acesso em 13 jul. 2009.

[8] Dantas, Mário. **Tecnologia de Redes de Comunicação e Computadores.** São Paulo: Axcel Books do Brasil, 2002. 328 p. ISBN 8573231696.

[9] Forouzan, Behrouz A. **Comunicação de Dados e Redes de Computadores**. 3ª ed. Porto Alegre: Bookman, 2006. 840 p. ISBN 8536306149.

[10] Zacker, Craig, Paul Doyle. **Redes de Computadores: Configuração, Manutenção e Expansão.** São Paulo: Makron Books, 2000. 1056 p. ISBN 8534609152.

[11] Frinhani, Rafael de Magalhães Dias. **Projeto de Reestruturação do Gerenciamento e Otimização da Rede Computacional da Universidade Federal de Lavras.** Lavras – MG, 2005. 90 p.

[12] Barros, Odair Soares. **Segurança de redes locais com a implementação de VLANS – O caso da Universidade Jean Piaget de Cabo Verde**. Disponível em http://bdigital.unipiaget.cv:8080 /dspace /bitstream/123456789/69/1/Odair%20Barros %20.pdf . Acesso em 18 ago. 2009.

[13] IEEE Standard P802.1 Q. **IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.** 30 de Julho de 1998. Disponível em : http://standards.ieee.org/getieee802/download/802.1Q-1998.pdf . Acesso em 22 jul. 2009.

[14] Jamhour, Edgard. **Vlans Ethernet.** Disponível em http://eureka.pucpr.br/repositorio/download.php?codLink=2068696 . Acesso em 13 mai. 2008.

[15] Sousa, Orlando, Nuno Pereira. **VLAN (Virtual Local Area Network).** Disponível em : http://www.dei.isep.ipp.pt/~npereira/aulas/asist/07/misc/aula8.pdf . Acesso em 22 jul. 2009.

[16] Guilherme, Willian. **CCNA – 640-802 – Protocolo VTP (Virtual Trunk Protocol).** Disponível em: http://www.netip-sec.com.br/?p=601 . Acesso em 18 set. 2009.

[17] Souza, Alessandro Goulart. **Spanning Tree Protocol.** Disponível em: http://si.uniminas.br/ TFC/monografias/Monografia%20Alessandro.pdf . Acesso em 13 set. 2009.

[18] Zacaron, Alexandro Marcelo. **Utilizando Recursos de Switching STP e Vlan.** Disponível em: http://www2.dc.uel.br/nourau/document/?down=562 . Acesso em 18 set. 2009.

[19] Jamhour, Edgard. **MetroEthernet.** Disponível em http://www.ppgia.pucpr.br/~jamhour/Pessoal /Especializacao/Atual/TARC/MetroEthernet.ppt. Acesso em 06 Out. 2009.

[20] Cisco Systems Inc. **Understanding Multiple Spanning Tree Protocol (802.1s).** Disponível em: http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfc.shtml# mst_region . Acesso em 06 out. 2009.